IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No.	10/748,053
Filing Date	December 30, 2003
Inventorship	Hamaski
Applicant/Appellant	Hewlett-Packard Company
Group Art Unit	2444
Examiner	BAYARD, Kjename M.
Confirmation No.	8338
Attorney's Docket No.	200701923-3

Title: Management of service components installed in an electronic device in a mobile services network

APPEAL BRIEF

To: MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

As required under 37 C.F.R. §41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on July 9, 2010, and is in furtherance to the Notice of Appeal.

This brief contains items under the following headings as required by 37 C.F.R. §41.37 and M.P.E.P. §1206:

I. Real Party In Interest
II. Related Appeals, Interferences, and Judicial Proceedings
III. Status of Claims
IV. Status of Amendments
V. Summary of Claimed Subject Matter
VI. Grounds of Rejection to be Reviewed on Appeal
VII. Argument
VIII. Claims Appendix
IX. Evidence Appendix
X. Related Proceedings Appendix

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P., a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 31 claims pending in this application (Claims 1-2 and 4-32).

B. Current Status of Claims

1. Claims canceled: 3.
2. Claims withdrawn from consideration but not canceled: none.
3. Claims pending: 1-2 and 4-32.
4. Claims allowed: none.
5. Claims rejected: 1-2 and 4-32.

C. Claims on Appeal

The claims on appeal are claims 1-2 and 4-32.

IV. STATUS OF AMENDMENTS

Appellant last amended the claims in an Amendment and Response filed on December 11, 2009, and these amendments were entered. Therefore the claims on appeal (as reflected in the claim appendix) are the claims presented in the Amendment and Response filed on December 11, 2009 and have already been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following is provided pursuant to Rule 41.37(c)(1)(v) which requires "a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, which shall refer to the specification by page and line number, and to the drawings if any, by reference characters." Nothing in this Section V should be construed to limit the scope of any of the claims involved in the appeal, which are enumerated in full in the Appendix to this Appeal Brief.

According to claim 1, a mobile services network (105 in FIG. 1, 205, in FIG. 2, 305 in FIG. 3, 405 in FIG. 4, 505 in FIG. 5; para. [0051], [0059], [0067], [0075]-[0076], [0085]) for management of service components in an electronic device (107 in FIG. 1, 207 in FIG. 2, 307 in FIG. 3, 407 in FIG. 4, 507 in FIG. 5; para. [0051]-[0056], [0059]-[0060], [0062], [0064]-[0065]), the mobile services network comprising: a plurality of regions (113, 115, 117, 119 in FIG. 1, 213, 215, 217, 219 in FIG. 2, 313, 315, 317, 319 in FIG. 3, 413, 415, 417, 419 in FIG. 4, 513, 515, 517, 519 in FIG. 5; para. [0051], [0059]-[0061], [0064]-[0065], [0069], [0075], [0077], [0089]) of data and content stored in non-volatile memory (111 in FIG. 1, 211 in FIG. 2, 311 in FIG. 3, 411 in FIG. 4, 511 in FIG. 5; para. [0056], [0071], [0075]) in the electronic device; a plurality of server-side components (125, 127, 129, 131 in FIG. 1, 225, 227, 229, 231 in FIG. 2, 325, 327, 329, 331 in FIG. 3, 425, 427, 429, 431 in FIG. 4, 525, 527, 529, 531 in FIG. 5; para. [0052], [0053], [0055]-[0056], [0062]-[0063], [0067]-[0070], [0076], [0079]-[0082], [0086], [0089]) each of the server-side components remotely managing at least one associated region of the plurality of regions of data and content in the non-volatile memory of the electronic device; and wherein remote access to each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms which execute on the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or

other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

According to claim 11, a mobile services network (105 in FIG. 1, 205, in FIG. 2, 305 in FIG. 3, 405 in FIG. 4, 505 in FIG. 5; para. [0051], [0059], [0067], [0075]-[0076], [0085]) comprising an electronic device (107 in FIG. 1, 207 in FIG. 2, 307 in FIG. 3, 407 in FIG. 4, 507 in FIG. 5; para. [0051]-[0056], [0059]-[0060], [0062], [0064]-[0065]) having access to a plurality of services, and wherein the electronic device being adapted to be managed remotely, the mobile services network comprising: a management server for managing access to a plurality of services associated with the electronic device; a plurality of service management repositories (125, 127, 129, 131 in FIG. 1, 225, 227, 229, 231 in FIG. 2, 325, 327, 329, 331 in FIG. 3, 425, 427, 429, 431 in FIG. 4, 525, 527, 529, 531 in FIG. 5; para. [0052], [0053], [0055]-[0056], [0062]-[0063], [0067]-[0070], [0076], [0079]-[0082], [0086], [0089]), each service management repository arranged to remotely manage at least one associated service component of a plurality of service components (113, 115, 117, 119 in FIG. 1, 213, 215, 217, 219 in FIG. 2, 313, 315, 317, 319 in FIG. 3, 413, 415, 417, 419 in FIG. 4, 513, 515, 517, 519 in FIG. 5; para. [0051], [0059]-[0061], [0064]-[0065], [0069], [0075], [0077], [0089]) installed in non volatile memory (111 in FIG. 1, 211 in FIG. 2, 311 in FIG. 3, 411 in FIG. 4, 511 in FIG. 5; para. [0056], [0071], [0075]) of the electronic device; and wherein secure access to each of the plurality of associated service components in the electronic device by a corresponding one of the plurality of service management repositories is controlled by an associated one of a plurality of security mechanisms which execute in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

According to claim 15, a mobile network (105 in FIG. 1, 205, in FIG. 2, 305 in FIG. 3, 405 in FIG. 4, 505 in FIG. 5; para. [0051], [0059], [0067], [0075]-[0076], [0085]) for updating firmware and software in an electronic device (107 in FIG. 1, 207 in FIG. 2, 307 in FIG. 3, 407 in FIG. 4, 507 in FIG. 5; para. [0051]-[0056], [0059]-[0060], [0062], [0064]-[0065]), the mobile network comprising: a management server facilitating management of firmware and software in the electronic device; a corporate virtual user group management server for corporate virtual user group management; a corporate software repository (131 in FIG. 1, 231 in FIG. 2, 331 in FIG. 3, 431 in FIG. 4, 531 in FIG. 5; para. [0052], [0053],

[0055]-[0056], [0062]-[0063], [0067]-[0070], [0076], [0079]-[0082], [0086], [0089]) being employed for corporate virtual user group management and for securely distributing corporate software and corporate data to at least one of a plurality of separate segments of non-volatile memory (111 in FIG. 1, 211 in FIG. 2, 311 in FIG. 3, 411 in FIG. 4, 511 in FIG. 5; para. [0056], [0071], [0075]) in the electronic device, the at least one segment associated with a particular user group; and wherein remote access to each of the plurality of segments of non-volatile memory by the management server is controlled by an associated one of a plurality of security mechanisms (117 in FIG. 1, 217 in FIG. 2, 317 in FIG. 3, 417 in FIG. 4, 517 in FIG. 5; para. [0051], [0059]-[0061], [0064]-[0065], [0069], [0075], [0077], [0089]) which execute in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

According to claim 25, a mobile services network (105 in FIG. 1, 205, in FIG. 2, 305 in FIG. 3, 405 in FIG. 4, 505 in FIG. 5; para. [0051], [0059], [0067], [0075]-[0076], [0085]) for managing firmware and software in an electronic device (107 in FIG. 1, 207 in FIG. 2, 307 in FIG. 3, 407 in FIG. 4, 507 in FIG. 5; para. [0051]-[0056], [0059]-[0060], [0062], [0064]-[0065]), the mobile services network comprising: a plurality of management servers (125, 127, 129, 131 in FIG. 1, 225, 227, 229, 231 in FIG. 2, 325, 327, 329, 331 in FIG. 3, 425, 427, 429, 431 in FIG. 4, 525, 527, 529, 531 in FIG. 5; para. [0052], [0053], [0055]-[0056], [0062]-[0063], [0067]-[0070], [0076], [0079]-[0082], [0086], [0089]) for managing different logical segments of non-volatile memory (111 in FIG. 1, 211 in FIG. 2, 311 in FIG. 3, 411 in FIG. 4, 511 in FIG. 5; para. [0056], [0071], [0075]) of the electronic device; the electronic device comprising non-volatile memory segmented into a plurality of logical segments (113, 115, 117, 119 in FIG. 1, 213, 215, 217, 219 in FIG. 2, 313, 315, 317, 319 in FIG. 3, 413, 415, 417, 419 in FIG. 4, 513, 515, 517, 519 in FIG. 5; para. [0051], [0059]-[0061], [0064]-[0065], [0069], [0075], [0077], [0089]) with a different one of the plurality of management servers associated with each of the plurality of logical segments; and wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or

other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

The summary is set forth in several exemplary embodiments that correspond to the independent claims. It is noted that no dependent claims containing means plus function are argued separately. Discussions about elements and recitations to these claims can be found at least at the cited locations in the specification and drawings.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) The Office Action rejected claims 1-2, 4-7, and 10-14 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Pub. No. 2002/0124007 to Zhao ("Zhao") in view of International Publication No. WO02/23925 to Weisshaar, et al. ("Weisshaar").
2) The Office Action rejected claim 13 under 35 U.S.C. 103(a) as being unpatentable over Zhao in view of Weisshaar and further in view of U.S. Patent Application No. 2004/0203593 to Whelan, et al. ("Whelan").
3) The Office Action rejected claims 15-27 and 32 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Pub. No. 2004/0002943 to Merrill, et al. ("Merrill") in view of Weisshaar.
4) The Office Action rejected claims 8-9 under 35 U.S.C. 103(a) as being unpatentable over Zhao in view of Weisshaar, and further in view of U.S. Patent Pub. No. 2003/0022657 to Herschberg, et al. ("Herschberg").
5) The Office Action rejected claims 28-31 under 35 U.S.C. 103(a) as being unpatentable over Merrill in view of Weisshaar, and further in view of Herschberg.

VII. ARGUMENT

Rejections under 35 U.S.C. §103(a)

In its decision, KSR Int'l Co. v. Teleflex, Inc., No 04-1350 (U.S. Apr. 30, 2007), the Supreme Court reaffirmed application of the Graham factors in making a determination of

obviousness under 35 U.S.C. § 103(a). The four factual inquiries under Graham are: (1) determining the scope and contents of the prior art; (2) ascertaining the differences between the prior art and the claims in issue; (3) resolving the level of ordinary skill in the pertinent art, and (4) evaluating evidence of secondary consideration. Even if all of the prior art elements are disclosed by separate prior art references, the Examiner still must identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed.

First Rejection under 35 U.S.C. §103(a)

Claims 1-2, 4-7, and 10-14 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Zhao in view of Weisshaar.

Independent Claim 1

Claim 1 recites in part "wherein remote access to each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms which execute on the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content."

The Examiner admits that the primary reference (Zhao) does not teach these recitations, and instead relies on Weisshaar at page 10, lines 32-33, the connection manager at page 11, lines 4-8, page 14, lines 31-33, page 36, lines 8-9, and the hot upgrade capability on page 19, lines 21-26. Appellant contends that the Examiner is simply citing to passing references of "security" and "updating" and saying that these brief mentions in the reference meet the burden of proof required under Section 103 to teach each of the specific recitations in the claim. Upon closer analysis of these passages, it is clear that:

"Security manager 234 provides permission and policy restraints within the client platform 200" Page 10.

"Connection manager 236 manages connections of the client platform 200 to one or more networks . . . . It can require security (e.g., authentication, encryption, etc.) as a precondition to a connecton. . . ." Page 11.

"One purpose of this invention is to provide a system to allow a mobile client platform to discover and use services that become available dynamically within the client platform . . . ." Page 14.

"Services are restricted to the same stringent security policies imposed by the application manager module 232." Page 36.

"The service registries are repositories for local services. Facilities are provided to add services to, remove services from, and alter services within the registry. Support of basic life-cycle management functions is provided. These can be used by services to provide a hot upgrade capabiluy. . . ." Page 19.

Notably, there is no teaching of the specific claim recitations of remote access to each of the plurality of regions of data and content in the electronic device being controlled by an associated one of a plurality of security mechanisms which execute on the electronic device to enable a particular one of the plurality of server-side components to do any of these things.

The Examiner is vague at best in his rejection and does not provide any reasoning for relying on these portions of Weisshaar. In order for the rejection make sense, Appellant surmises that the Examiner interprets the services being restricted to the same security policies imposed by the application manager module (page 36 quoted above) as teaching remote access being controlled by a security mechanism in the claim. However, even with this understanding of the vague rejection, the disclosure in Weisshaar of services being restricted to the same security policies imposed by the application manager **teaches against the claim recitations**, which require access to be controlled by an associated one of a plurality of security mechanisms - not the same security policy as disclosed on page 36 in Weisshaar.

Therefore, the Examiner has failed to establish that independent claim 1 is unpatentable in view of the cited references.

Dependent Claims 2, 5-7, and 10

Claims 2, 5-7, and 10 depend from claim 1, which is believed to be allowable. Therefore, claims 2, 5-7, and 10 are also believed to be allowable for at least the same reasons as claim 1.

Dependent Claim 4

Claim 4 depends from claim 1, which is believed to be allowable. Therefore, claim 4 is also believed to be allowable for at least the same reasons as claim 1.

In addition, the recitations argued above for claim 1 are further narrowed in dependent claim 4, which states "wherein the plurality of regions of data and content in the electronic device comprise: a corporation related data and content region being managed by a corporate server-side component; an end-user related data and content region being managed by an end-user related server-side component; an operator related data and content region being managed by an operator related server-side component; and a manufacturer related data and content region being managed by a manufacturer related server-side component.

The Examiner relies vaguely on Zhao (para. 35, 42, and 48) as teaching each of these regions of data and content. These paragraphs are each reproduced below, with highlighted areas showing what the Appellant surmises that the Examiner is interpreting as being each of the claim recitations (although the rejection itself is not clear):

[0035] The device index (Dev_Index) preferably lists an index to intelligent device 15A, in Intranet 16. In a preferred embodiment, the Dev_Index (Dev_Index) stores the name of intelligent device 15A. The device digital identifier (Dev_ID) stores a digital identifier uniquely identifies intelligent device 15A. Typically, ***the device digital identifier is set by the manufacturer of intelligent device 15A.*** *In order to access intelligent device 15A, a client is preferably required to provide a security code matching the device security code (Dev_Sec) in device 40 of device index table 32. The device communication route (Dev_Rt) preferably specifies device communication*

protocol, port, address or telephone number, and communication speed for intelligent device 15A. ***[The Examiner cites to this as being the manufacturer related data and content managed by a manufacturer related server side component].***

[0042] As shown in FIG. 5, device property table 50 includes a device digital identifier (Dev_ID). Preferably, the device digital identifier (Dev_ID) in device property table 50 is the same as that in device 40 in device index table 32. The device digital identifier establishes the one to one correspondences between device 40 in device index table 32 and device property table 50. Device property table 50 preferably also includes a device descriptor (Dev_DSP) that describes byte length of the address code of intelligent device 15A and data transmission mode, e.g., higher byte first or lower byte first, between network server 20 and intelligent device 15A. Device property table 50 further includes a device object number (Dev_Obj_NUM) that indicates the number of objects associated with intelligent device 15A. For each object, device property table 50 preferably includes an object name (Dev_Obj_1, Dev_Obj_2, Dev_Obj_i). Referring back to FIG. 3, the object names in device property table 35A point to corresponding object property tables (A1, A2. . . . , Ai) in database 30 associated with intelligent device 15A. Likewise, the object names in device property table 35B point to corresponding object property tables (B1, B2, ... Bj) in database 30 associated with intelligent device 15B. Further, the object names in device property table 35N point to corresponding object property tables (N1, N2. . . . Nk) in database 30 associated with intelligent device 15N. ***[Although the Examiner cites to this as being the corporation related data and content region being managed by a corporate server-side component, there does not appear to be anything here that would teach these recitations].***

[0048] A constant is generally used for describing a fixed parameter object such as, for example, the name, serial number, model number, edition, number, protocol, etc. of intelligent device 15A. In this context, the constant functions as an object identifier. The constant can also include parameters for ***describing other object characteristics as defined by the user****. The constant is preferably a read only data in order to maintain its constancy.* ***[The Examiner cites to this as disclosing an end-user related data and content region being managed by an end-user related server-side component].***

The Examiner is stretching his interpretation of the reference beyond its clear teachings. The reference does not teach these very specific data and content regions. Even ignoring these very specific data and content regions, which is error itself, there is still no teaching that these regions are managed by the respective server-side components. In addition, the Examiner provided no support in the reference for rejecting an operator related data and content region being managed by an operator related server-side component.

Therefore, the Examiner has failed to establish that dependent claim 4 is unpatentable in view of the cited references.

Independent Claim 11

Claim 11 recites "wherein secure access to each of the plurality of associated service components in the electronic device by a corresponding one of the plurality of service management repositories is controlled by an associated one of a plurality of security mechanisms which execute in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content." The cited combination fails to disclose at least these recitations for the reasons discussed above for claim 1.

Therefore, the Examiner has failed to establish that independent claim 11 is unpatentable in view of the cited references.

Dependent Claims 12 and 14

Claims 12 and 14 depend from claim 11, which is believed to be allowable. Therefore, claims 12 and 14 are also believed to be allowable for at least the same reasons as claim 11.

Dependent Claim 13

Claim 13 depends from claim 11, which is believed to be allowable. Therefore, claim 13 is also believed to be allowable for at least the same reasons as claim 11. Claim 13 also includes similar recitations as claim 4. Therefore, claim 13 is believed to be allowable for the additional reasons argued above for claim 4.

Second Rejection under 35 U.S.C. §103(a)

Claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Zhao in view of Weisshaar and further in view of Whelan.

Dependent Claim 13

Claim 13 depends from claim 11, which is believed to be allowable. Therefore, claim 13 is also believed to be allowable for at least the same reasons as claim 11.

Third Rejection under 35 U.S.C. §103(a)

Claims 15-27 and 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Merrill in view of Weisshaar.

Independent Claim 15

Claim 15 recites "wherein remote access to each of the plurality of segments of non-volatile memory by the management server is controlled by an associated one of a plurality of security mechanisms which execute in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.." The cited combination fails to disclose at least these recitations for the reasons discussed above for claim 1.

Therefore, the Examiner has failed to establish that independent claim 15 is unpatentable in view of the cited references.

Dependent Claim 16

Claim 16 depends from claim 11, which is believed to be allowable. Therefore, claim 16 is also believed to be allowable for at least the same reasons as claim 11.

In addition, claim 16 further recites "a digital rights management server for disseminating rights to use corporate software and corporate data disseminated by the corporate virtual user group management server." The Examiner relies on Merrill at para. [0099]-[0100], which are reproduced below:

> *[0099] In an action 516, to ensure that mobile client application downloads remain secure, file verification and user authorization component 434 checks the digital signature (i.e., the claimed identity) of the received download instructions against one or more trusted source(s) from which download instructions are considered to be secure and reliable. Such trusted sources are stored in TSL 428. For instance, the TSL is a listing of trusted application delivery servers and their public keys. Scheduling component 308 exposes one or more interfaces via scheduler API 430 to update and otherwise manage contents of the TSL. An exemplary scheduler API 430 is shown below in APPENDIX A.*
>
> *[0100] In one implementation, TSL 428 includes an X.600 certificate for the management server 302 which includes an RDN (name), public key, etc. Although a certificate in the TSL may be purposefully or accidentally deleted from the TSL, such a deleted certificate cannot simply be replaced with another key. This ensures that mobile client 304 application delivery remains secure. Additionally, even if a particular trusted source certificate is purposefully or accidentally deleted from the TSL, as long as a portion of non-volatile memory of the mobile client is so preconfigured, a cold boot of mobile client 304 can re-instate the deleted certificate.*

Again, the Examiner's rejection is vague, without any explanation of what specifically in these passages is being relied on as teaching the specific claim recitations. In any event, while these passages disclose user authorization, Appellant cannot find any support in these passages for upholding the rejection of the specific claim recitations of a

digital rights management server for disseminating rights to use corporate software and corporate data disseminated by the corporate virtual user group management server.

Dependent Claim 17

Claim 17 depends from claim 11, which is believed to be allowable. Therefore, claim 16 is also believed to be allowable for at least the same reasons as claim 11.

In addition, claim 17 further recites "a corporate data segment for storing and managing corporate software and corporate data in non-volatile memory, wherein management of the corporate data segment being conducted solely by the corporate virtual user group management server." The Examiner relies on Merrill at para. [0062], which is reproduced below:

> *[0062] The mobile client device 304 also has program memory 424 into which downloaded applications are installed, a database or other data structure 426 in which client device 304 maintains or caches an offering list indicating applications or packages that have already been made available to the client device through previous interactions with management server 302, and a trusted source list ("TSL") 428 for authenticating download instructions 410 received from management server 302. The offering list is available for presentation to a user of the remote client independent of any connection to the management server. The remote client is configured to automatically remove an offering from the offerings list responsive to download and installation of the offering onto the remote client.*

Again, the Examiner's rejection is vague, without any explanation of what specifically in these passages is being relied on as teaching the specific claim recitations. In any event, while these passages disclose an offering list indicating applications or packages that have already been made available, Appellant cannot find any support in these passages for upholding the rejection of the specific claim recitations of a corporate data segment for storing and managing corporate software and corporate data in non-volatile memory, wherein management of the corporate data segment being conducted solely by the corporate virtual user group management server.

Dependent Claim 18

Claim 18 depends from claim 11, which is believed to be allowable. Therefore, claim 18 is also believed to be allowable for at least the same reasons as claim 11.

Dependent Claims 19-24

Claims 19-24 depend from claim 15, which is believed to be allowable. Therefore, claims 19-24 are also believed to be allowable for at least the same reasons as claim 15.

Independent Claim 25

Claim 25 recites "wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content." The cited combination fails to disclose at least these recitations for the reasons discussed above for claim 1.

Therefore, the Examiner has failed to establish that independent claim 25 is unpatentable in view of the cited references.

Dependent Claims 26-27 and 32

Claims 26-27 and 32 depend from claim 25, which is believed to be allowable. Therefore, claims 26-27 and 32 are also believed to be allowable for at least the same reasons as claim 25.

Fourth Rejection under 35 U.S.C. §103(a)

Claims 8-9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Zhao in view of Weisshaar, and further in view of Herschberg.

Dependent Claims 8-9

Claims 8-9 depend from claim 1, which is believed to be allowable. Therefore, claims 8-9 are also believed to be allowable for at least the same reasons as claim 1.

Fifth Rejection under 35 U.S.C. §103(a)

Claims 28-31 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Merrill in view of Weisshaar, and further in view of Herschberg.

Dependent Claim 28

Claims 28 depends from claim 25, which is believed to be allowable. Therefore, claim 28 is also believed to be allowable for at least the same reasons as claim 25.

In addition, claim 28 further recites "a corporate data and software segment, and the electronic device being associated with a corporate user membership for an employee of a corporation, wherein the corporate data management server being adapted to erase at least a portion of the corporate data and software segment on the electronic device when the employee of the corporation associated with the electronic device severs an employment relationship." The Examiner relies vaguely on Herschberg at para. [0095], reproduced below:

> *[0095] When a user logs on to server framework 104, the system determines what downloaded applications 204 are resident on the user's device and automatically downloads to the user any "required" applications that the user does not have that are compatible with the user's device. In addition, the system provides the user the option to download any "grant" applications. Finally, the system deletes from the user's device any "unauthorized" applications. In this way, the system ensures that the user has an appropriate set of applications on his or her device 106.*

Again, the Examiner's rejection is vague, without any explanation of what specifically in these passages is being relied on as teaching the specific claim recitations. In any event, while Herschberg discloses determining what downloaded applications are

resident on the user's device and automatically downloading any required applications. Appellant cannot find any support in these passages for upholding the rejection of the specific claim recitations of the electronic device being associated with a corporate user membership for an employee of a corporation. In addition, while Herschberg discloses deleting unauthorized applications, this is not the same as the claim recitation of the corporate data management server being adapted to erase at least a portion of the corporate data and software segment on the electronic device when the employee of the corporation associated with the electronic device severs an employment relationship.

Dependent Claim 29

Claims 29 depends from claim 25, which is believed to be allowable. Therefore, claim 29 is also believed to be allowable for at least the same reasons as claim 25.

In addition, claim 29 further recites "wherein the electronic device comprises a corporate data and software segment, and the electronic device being associated with a corporate user membership for an employee of a corporation, the corporate data management server being adapted to disable the electronic device when the employee of the corporation associated with the electronic device severs an employment relationship." The Examiner relies on Herschberg at para. [0095] already reproduced above, and para. [0116], reproduced below:

> *[0116] As will be recognized, FIG. 1 shows a preferred embodiment of the user properties dialog when the user tab 1102 is selected. As shown in FIG. 11, panel 1112 preferably displays information concerning the user including his or her name, username, last login, description, whether the user's account is active, and whether the user has administrator rights. In a preferred embodiment, each user's account is initially designated "active." However, an administrator may change that status to "disabled" to temporarily block login access to a particular user. The system may also automatically change this setting to "disabled" if the administrator sets up a system option of blocking access after a number of successive failed login attempts.*

Again, the Examiner's rejection is vague, without any explanation of what specifically in these passages is being relied on as teaching the specific claim recitations. In

any event, while Herschberg discloses deleting unauthorized applications, this is not the same as the claim recitation of the corporate data management server being adapted to disable the electronic device when the employee of the corporation associated with the electronic device severs an employment relationship.

Dependent Claim 30

Claims 30 depends from claim 25, which is believed to be allowable. Therefore, claim 30 is also believed to be allowable for at least the same reasons as claim 25.

In addition, claim 30 further recites "a corporate data and software segment, and the electronic device being associated with a corporate user membership for an employee of a corporation, wherein the corporate data management server is adapted to disable access to the corporate data and software segment of the electronic device to prevent unauthorized access to the corporate data segment in the electronic device." The Examiner relies on para. [0116] already reproduced above, and para. [0092], reproduced below:

> *[0092] "Deny" applications are applications that are not permitted for a particular user or members of particular user groups. For example, continuing with the example from above, if the administrator identifies the spreadsheet application as "unauthorized" for users in the engineering user group, users belonging to that group would not be permitted to download the application.*

Again, the Examiner's rejection is vague, without any explanation of what specifically in these passages is being relied on as teaching the specific claim recitations. In any event, while Herschberg discloses denying application that are not permitted for a particular user or members of particular user groups, this is not the same as the claim recitation of wherein the corporate data management server is adapted to disable access to the corporate data and software segment of the electronic device to prevent unauthorized access to the corporate data segment in the electronic device.

Dependent Claim 31

Claims 31 depends from claim 25, which is believed to be allowable. Therefore, claim 31 is also believed to be allowable for at least the same reasons as claim 25.

Conclusion

For the reasons provided herein, Appellant respectfully requests the Board to rule that the rejections of the claims are improper.

Respectfully Submitted,

/Mark D. Trenner/

Dated: September 9, 2010 By: _____

Mark D. Trenner
Reg. No. 43,961
(720) 221-3708

VIII. CLAIMS APPENDIX

1. A mobile services network for management of service components in an electronic device, the mobile services network comprising:

a plurality of regions of data and content stored in non-volatile memory in the electronic device;

a plurality of server-side components, each of the server-side components remotely managing at least one associated region of the plurality of regions of data and content in the non-volatile memory of the electronic device; and

wherein remote access to each of the plurality of regions of data and content in the electronic device is controlled by an associated one of a plurality of security mechanisms which execute on the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

2. The mobile services network according to claim 1, wherein the plurality of server-side components further comprise:

a plurality of repositories providing data and content for the electronic device, each of the plurality of repositories being capable of managing at least one region of data and content in the electronic device.

3. (Cancelled)

4. The mobile services network according to claim 1, wherein the plurality of regions of data and content in the electronic device comprise:

a corporation related data and content region being managed by a corporate server-side component;

an end-user related data and content region being managed by an end-user related server-side component;

an operator related data and content region being managed by an operator related server-side component; and

a manufacturer related data and content region being managed by a manufacturer related server-side component.

5. The mobile services network according to claim 1, further comprising:

a management server for managing the electronic device, wherein the plurality of server-side components manage the plurality of regions of data and content in the electronic device via the management server.

6. The mobile services network according to claim 5, wherein each of the plurality of server-side components are adapted to manage creating, updating, deleting, and configuring at least a corresponding one of the plurality of regions of data and content.

7. The mobile services network according to claim 6, wherein each of the plurality of server-side components is associated with a corresponding region of the plurality of regions of data and content and each of the plurality of server-side components is further adapted to manipulate and manage the corresponding region.

8. The mobile services network according to claim 7, wherein the plurality of regions of data and content further comprise:

a firmware region managed by a management server which is managed by a wireless operator;

an operating system region managed by the wireless operator;

a corporate logos region managed by a corporate user access management server;

a corporate confidential data and software region managed by the corporate user access management server; and

a user data region managed by the end-user.

9. The mobile services network according to claim 8, wherein each of the plurality of regions of data and content comprise at least one update agent associated therewith for updating data and content, and wherein the at least one update agent is adapted to add, delete, configure, update, and manage associated regions of the plurality of regions of data and content.

10. The mobile services network according to claim 1, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

11. A mobile services network comprising an electronic device having access to a plurality of services, and wherein the electronic device being adapted to be managed remotely, the mobile services network comprising:

a management server for managing access to a plurality of services associated with the electronic device;

a plurality of service management repositories, each service management repository arranged to remotely manage at least one associated service component of a plurality of service components installed in non volatile memory of the electronic device; and

wherein secure access to each of the plurality of associated service components in the electronic device by a corresponding one of the plurality of service management repositories is controlled by an associated one of a plurality of security mechanisms which execute in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

12. The mobile services network according to claim 11, wherein the associated service components comprise:

at least one firmware and operating system layer;

a communication stack;

corporate data; and

end-user personal data, wherein each of the associated service components employ a corresponding security service available in the electronic device.

13. The mobile services network according to claim 12, wherein the plurality of service management repositories further comprise:

a corporate management server and repository for managing corporate data in the electronic device;

an operator management server and repository for managing the communication stack in the electronic device;

a manufacturer management server and repository for managing the at least one firmware and operating system layer in the electronic device; and

an end-user management server and repository for managing end-user personal data in the electronic device.

14. The mobile services network according to claim 11, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

15. A mobile network for updating firmware and software in an electronic device, the mobile network comprising:

a management server facilitating management of firmware and software in the electronic device;

a corporate virtual user group management server for corporate virtual user group management;

a corporate software repository being employed for corporate virtual user group management and for securely distributing corporate software and corporate data to at least one of a plurality of separate segments of non-volatile memory in the electronic device, the at least one segment associated with a particular user group; and

wherein remote access to each of the plurality of segments of non-volatile memory by the management server is controlled by an associated one of a plurality of security mechanisms which execute in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

16. The mobile network according to claim 15, further comprising a digital rights management server for disseminating rights to use corporate software and corporate data disseminated by the corporate virtual user group management server.

17. The mobile network according to claim 16, wherein the electronic device further comprises:

non-volatile memory; and

a corporate data segment for storing and managing corporate software and corporate data in non-volatile memory, wherein management of the corporate data segment being conducted solely by the corporate virtual user group management server.

18. The mobile network according to claim 16, further comprising:

the corporate software repository being employed to update corporate software and corporate data in the corporate data segment in non-volatile memory of the electronic device; and

an update package repository being employed to retrieve update packages for updating firmware and software in the electronic device.

19. The mobile network according to claim 18, wherein software in the electronic device comprises:

an operating system; and

a plurality of applications updateable by the management server.

20. The mobile network according to claim 15, wherein the electronic device comprises one of mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

21. A method of managing a corporate data segment in an electronic device, the method comprising:

retrieving corporate software and corporate data from a corporate data repository and facilitating retrieval via a corporate virtual user group management server;

storing retrieved corporate software and corporate data in a corporate data segment of the electronic device;

retrieving rights to access or execute corporate software and corporate data from a digital rights management server;

updating the corporate data segment;

wherein the electronic device comprises a plurality of logically separate data segments; and

wherein remote access to each of the plurality of data segments by a corresponding one of a plurality of data repositories is controlled by an associated one of a plurality of security mechanisms in the electronic device.

22. The method according to claim 21, further comprising:

incorporating verification information in corporate software and corporate data retrieved from the corporate data repository; and

updating the corporate data segment in the electronic device only after verification of the verification information.

23. The method according to claim 22, further comprising:

incorporating end-user authentication information in corporate software and corporate data during retrieval from the corporate data repository.

24. The method according to claim 21, wherein the electronic device comprises one of mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

25. A mobile services network for managing firmware and software in an electronic device, the mobile services network comprising:

a plurality of management servers for managing different logical segments of non-volatile memory of the electronic device;

the electronic device comprising non-volatile memory segmented into a plurality of logical segments with a different one of the plurality of management servers associated with each of the plurality of logical segments; and

wherein remote access to each of the plurality of logical segments of non-volatile memory by a corresponding one of a plurality of management servers is controlled by an associated one of a plurality of security mechanisms in the electronic device to enable a particular one of the plurality of server-side components to update code, data, service configuration information or other types of content in the at least one associated region in non-volatile memory of the plurality of regions of data and content.

26. The mobile services network according to claim 25, wherein the plurality of management servers employing digital rights management for security and for authorizing access to an associated one of the plurality of logical segments in the electronic device.

27. The mobile services network according to claim 26, wherein the plurality of segments comprise a corporate data and software segment being associated with a corporate data management server being one of the plurality of management servers.

28. The mobile services network according to claim 27, wherein the electronic device comprises a corporate data and software segment, and the electronic device being associated with a corporate user membership for an employee of a corporation, wherein the corporate data management server being adapted to erase at least a portion of the corporate data and software segment on the electronic device when the employee of the corporation associated with the electronic device severs an employment relationship.

29. The mobile services network according to claim 27, wherein the electronic device comprises a corporate data and software segment, and the electronic device being associated with a corporate user membership for an employee of a corporation, the corporate data management server being adapted to disable the electronic device when the employee of the corporation associated with the electronic device severs an employment relationship.

30. The mobile services network according to claim 27, wherein the electronic device comprises a corporate data and software segment, and the electronic device being associated with a corporate user membership for an employee of a corporation, wherein the corporate data management server is adapted to disable access to the corporate data and software segment of the electronic device to prevent unauthorized access to the corporate data segment in the electronic device.

31. The mobile services network according to claim 27, wherein the electronic device is associated with end-user membership in a user group, and the electronic device comprises an end-user data and software segment, the end-user data and software segment comprising:

a plurality of gaming software and address book data; and

an end-user data and software management server, the end-user data and software management server facilitating management of the end-user data and software segment;

facilitating membership to the user group, and

authorizing access to the end-user data and software segment by at least one of a plurality of management servers.

32. The mobile services network according to claim 25, wherein the electronic device comprises one of mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

IX. EVIDENCE APPENDIX

Not applicable.

X. RELATED PROCEEDINGS APPENDIX

Not applicable.